

CLAIM AMENDMENTS

This listing of claims will replace all prior versions, and listings, of claims in the application.

- 1 1-7. (Cancelled)
- 1 8. (Original) A method for authenticating the identity of a person comprising:  
2 obtaining baseline samples of biometric data from the person;  
3 forming a baseline profile from the biometric data;  
4 repeatedly obtaining additional biometric data from the person in  
5 response to the person accessing a portable device for information comprising  
6 time of day;  
7 comparing the additional data to the baseline profile for authenticating  
8 identity of the person; and  
9 developing a response to said comparing.
- 1 9. (Original) The method according to claim 8, wherein said accessing  
2 comprises the person pressing a button on the portable device ~~information~~  
3 ~~comprises time of day~~.
- 1 10. (Original) The method according to claim 9, wherein said portable device  
2 is wrist-worn.
- 1 11. (Original) The method according to claim 8, wherein said obtaining  
2 baseline samples comprises obtaining an image of the person's face.
- 1 12. (Original) The method according to claim 11, wherein said obtaining  
2 baseline samples comprises obtaining an image of the person's iris.
- 1 13. (Original) The method according to claim 8, wherein said obtaining  
2 baseline samples comprising obtaining a fingerprint image of the person.

1 14. (Original) The method according to claim 8, further comprising  
2 performing a superresolution algorithm on the baseline samples.

1 15. (Original) The method according to claim 14, further comprising  
2 communicating the baseline samples from the portable device to an external  
3 computer system, wherein said performing the superresolution algorithm is  
4 performed in the external computer system.

1 16. (Original) The method according to claim 15, wherein the external  
2 computer system performs said comparing the additional data to the baseline  
3 samples.

1 17. (Original) The method according to claim 15, further comprising  
2 upgrading a superresolution algorithm stored in the external computer.

1 18. (Original) The method according to claim 8, said comparing being by the  
2 portable device.

1 19. (Original) The method according to claim 8, said comparing being a  
2 computer system that is external to the portable device.

1 20. (Original) The method according to claim 19, wherein the external  
2 computer system includes mass storage for storing the additional biometric  
3 data.

1 21. (Original) The method according to claim 8, wherein the response  
2 disallows a transaction attempted by the wearer.

1 22. (Original) The method according to claim 21, said comparing  
2 comprising:  
3 forming a level of confidence that the identity of the person is correct;  
4 and  
5 comparing the level of confidence to predetermined minimum  
6 threshold level.

1 23. (Original) The method according to claim 22, said predetermined  
2 minimum threshold being for a particular transaction attempted by the person.

1 24. (Original) The method according to claim 21, further comprising sensing  
2 that the device is not being worn by the person and developing the response  
3 when the device is not being worn by the person.

1 25. (Original) The method according to claim 24, said sensing that the device  
2 is not being worn by the person comprising sensing a body temperature of the  
3 person.

1 26. (Original) The method according to claim 25, said sensing that the device  
2 is not being worn by the person comprising sensing a bio-noise of the person.

1 27. (Original) The method according to claim 8, further comprising:  
2 sensing environmental information; and  
3 including the environmental information in the baseline profile.

1 28. (Original) The method according to claim 27, wherein said environmental  
2 information comprises geographic location.

1 29. (Original) The method according to claim 8, further comprising updating  
2 the baseline sample by the additional biometric data when the additional  
3 biometric data successfully authenticates the identity of the person.

1 30. (Previously Presented) A method for authenticating the identity of a  
2 person comprising:  
3 obtaining baseline samples of biometric data from the person over a  
4 period of at least one day, the baseline samples being collected while the  
5 person goes about his or her normal activities;  
6 forming a baseline profile from the biometric data;  
7 repeatedly obtaining additional biometric data from the person;

8 comparing the additional data to the baseline profile for authenticating  
9 identity of the person; and  
10 developing a response to said comparing.

1 31. (Original) The method according to claim 30, further comprising freezing  
2 the baseline profile after said obtaining baseline samples.

1 32. (Original) The method according to claim 30, further comprising  
2 updating the baseline sample by the additional biometric data when the  
3 additional biometric data successfully authenticates the identity of the person.

1 33. (Original) The method according to claim 30, wherein the response  
2 disallows a transaction attempted by the wearer.

1 34. (Cancelled)

1 35. (Original) The method according to claim 30, wherein said obtaining  
2 baseline samples comprises obtaining an image of the person's face.

1 36. (Original) The method according to claim 35, wherein said obtaining  
2 baseline samples comprises obtaining an image of the person's iris.

1 37. (Original) The method according to claim 30, wherein the baseline  
2 samples include voice samples of the person.

1 38. (Previously Presented) A method for authenticating the identity of a  
2 person comprising:  
3 obtaining baseline samples of biometric data from the person over a  
4 period of at least one day;  
5 forming a baseline profile from the biometric data;  
6 repeatedly obtaining additional biometric data from the person;  
7 comparing the additional data to the baseline profile for authenticating  
8 identity of the person; and

9 updating the baseline sample by the additional biometric data when the  
10 additional biometric data successfully authenticates the identity of the person.